Preetha Chakrabarti
Rachel Elaine Hsu (*pro hac vice* forthcoming)
CROWELL & MORING LLP
Two Manhattan West
375 Ninth Avenue
New York, NY 10001
Telephone: (212) 223-4000
Facsimile: (212) 223-4134
pchakrabarti@crowell.com
rhsu@crowell.com

Anna Z. Saber (*pro hac vice* forthcoming)
CROWELL & MORING LLP
3 Embarcadero, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Facsimile: (415) 986-2827
asaber@crowell.com

Attorneys for Plaintiff Red Sense LLC

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

Red Sense LLC

Plaintiff,

v.

Yelisey Bohuslavskiy,
a.k.a. Elisei Boguslavskii

Defendant.

Civil Action No. 2:25-cv-12281

COMPLAINT AND DEMAND FOR JURY TRIAL

REDACTED PURSUANT TO L. CIV. R. 5.3

Plaintiff Red Sense LLC ("RedSense"), a Wyoming limited liability company with its principal place of business at One Boston Place, Suite 2600, Boston, Massachusetts 02018, brings this Complaint against Defendant Yelisey Bohuslavskiy ("Defendant" or "Bohuslavskiy"), an individual who RedSense is informed and believes resides at 7000 JFK Boulevard E, Apt. 42D, Guttenberg, New Jersey 07093, asserting claims for False Advertising under the Lanham Act, 15 U.S.C. § 1125, Tortious Interference with Contractual Relations, Tortious Interference with Prospective Contract, Trade Secret Misappropriation under the Defend Trade Secret Act, 18 U.S.C. § 1836 *et seq.*, Fraud, Conversion, Unjust Enrichment, Declaratory Relief pursuant to 22 U.S.C. § 2201, and Breach of Fiduciary Duty. RedSense alleges as follows:

INTRODUCTION

1. On February 24, 2025, when Bohuslavskiy announced his resignation as Chief Research Officer of RedSense, he threatened to notify all of RedSense's current and prospective customers that the services the customers were contracting with RedSense to provide would no longer be offered by RedSense, and would instead be offered exclusively through Bohuslavskiy via Affix Advisory, LLC, Bohuslavskiy's single-member LLC ("Affix"). In short, it was not enough for Bohuslavskiy to announce his resignation; he wanted to destroy the RedSense customer relationships, steal the business away from RedSense for his own

financial gain, and decimate the confidence customers had in RedSense to protect their cybersecurity concerns. And within days, these threats turned to action, as Bohuslavskiy methodically and persistently contacted RedSense customer after customer (using a personal Gmail email address), including RedSense's largest customers, where he raised vague "ethical" concerns about RedSense as a business, claimed that only he and his team (and, crucially, not RedSense) could provide the cybersecurity services that the customers had been paying RedSense to provide, that unless the customer began working with Bohuslavskiy directly (instead of RedSense) the customer was at great risk of cybersecurity threats, and that RedSense was not equipped to service these relationships.

2. Understandably, these customers were alarmed to receive such communications—the language used in these communications by Bohuslavskiy mirrored the language and tactics commonly used by cybercriminals or hackers in connection with phishing schemes, designed to trick the recipient into providing sensitive information that can then be used to unlawfully infiltrate computer systems. Customers, including RedSense's largest customers, began reaching out to RedSense, expressing concern and confusion. In particular, the customers did not know if this was a scam, if RedSense had been compromised, if Bohuslavskiy was speaking on behalf of RedSense (although Bohuslavskiy stated in his email that he had resigned as Chief Research Officer, his email contained numerous

references that he was still affiliated with RedSense), whether this dispute with Bohuslavskiy was indicative of RedSense's instability, and whether this dispute with Bohuslavskiy would undermine RedSense's ability to continue to provide valuable cybersecurity services to its customers. Prospective customers actively engaged in sales conversations with RedSense expressed that until this situation was resolved, they did not feel comfortable bringing their cybersecurity business to RedSense.

3. Concerned about the impact that Bohuslavskiy's conduct would have on RedSense's customer relationships and financial condition, RedSense immediately demanded that Bohuslavskiy cease and desist such communications with RedSense customers. This only emboldened Bohuslavskiy; his response to RedSense leadership was to threaten, "I will be informing each customer about this illegal action tomorrow, as well as what lead [sic] to it. With all screenshots and evidence attached." And then, he continued to contact customers repeatedly (often multiple times a week). Bohuslavskiy has ignored all requests to halt this destructive conduct, and to date continues to contact RedSense customers.

4. RedSense's investigation of Bohuslavskiy following his resignation has only revealed more troubling conduct. Bohuslavskiy served as RedSense's Chief Research Officer where he was responsible for day-to-day management of the threat research business function, budget, and resourcing. This involved him

working with third party vendors to procure assets for RedSense, such as source code these vendors developed, threat intelligence, and other deliverables that RedSense would ultimately incorporate into the services it provided to its customers. Bohuslavskiy was responsible for managing these vendors, which included managing and approving payments to these vendors for the work they performed. The problem? As RedSense discovered during their investigation, Bohuslavskiy was responsible for approving payments for work product that was either never completed or never provided to RedSense. And, given Bohuslavskiy's responsibilities for these vendors, he was in a position to know that these vendors were being improperly paid. In some instances, Bohuslavskiy even approved duplicate invoices, invoices on Affix paper and the original vendor invoices meaning that he was submitting requests to pay these vendors potentially *double* for work product that RedSense does not have any access to. If the work was performed, he hid RedSense intellectual property and other assets away from RedSense. If the work was not performed, Bohuslavskiy was complicit in a fraudulent scheme to steal from RedSense, deplete its funds, and cause it financial harm, all so that Bohuslavskiy and his team could line their pockets by obtaining payment for work never performed.

5. As if that were not bad enough, simultaneous to Bohuslavskiy's resignation, RedSense became aware that the systems used by him and his team

were accessed, any existing source code was copied out, and the file system was destroyed. RedSense's investigation into the incident revealed the credentials used to access the systems belonged to those RedSense provided to Igor Dmitriev ("Dmitriev"), Bohuslavskiy's brother and a RedSense Strategic Consultant, who Bohuslavskiy managed directly. Given the timing and the use of Dmitriev's credentials, RedSense is informed and believes, and on that basis alleges, that this theft of RedSense property was done by or at the direction, request, or encouragement of Bohuslavskiy.

6. This Complaint seeks to redress Bohuslavskiy's wrongs.

THE PARTIES

7. Plaintiff RedSense is, and all times mentioned herein was, a Wyoming limited liability company organized under the laws of the state of Wyoming. RedSense's principal place of business is located at One Boston Place, Suite 2600, Boston, Massachusetts 02018. RedSense delivers actionable, context-rich threat intelligence to its customers, which can be leveraged by its customers to strengthen detection and response capabilities and enhance the ability to prevent and remediate cyber threats.

8. Defendant Yelisey Bohuslavskiy, a.k.a. Eliseii Boguslavskii, is an individual who, RedSense is informed and believes, and on that basis alleges, resides in Guttenberg, New Jersey. From January 25, 2023 through February 24,

2025, Bohuslavskiy served as RedSense's Chief Research Officer until his resignation.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction under 28 U.S.C. § 1331, which provides jurisdiction over all actions brought pursuant to the laws of the United States, because RedSense is asserting claims which arise under the Defend Trade Secrets Act, 18 U.S.C. § 1836 *et seq*. and the Lanham Act, 15 U.S.C. §1051 *et. seq*. This Court has supplemental jurisdiction over the remaining state law claims asserted herein under 28 U.S.C. § 1367.

10. This Court has personal jurisdiction over Bohuslavskiy because RedSense is informed and believes (based on the information provided by Bohuslavskiy to RedSense in connection with his tax return), and on that basis alleges, that he is a resident of the State of New Jersey.

11. Venue is proper in the District of New Jersey, Newark vicinage pursuant to 28 U.S.C. § 1391(b)(1) because RedSense is informed and believes, and on that basis alleges, that Bohuslavskiy resides in the State of New Jersey and specifically within the boundary lines of the Newark vicinage.

GENERAL ALLEGATIONS

A. RedSense's Business

12. RedSense delivers cyber threat intelligence that is proactive, targeted, and made easy for its customers. RedSense empowers organizations to stay ahead of evolving cyber threats with a flexible, defense-grade solution tailored to meet unique needs without the complexity of traditional approaches. RedSense offers its customers a variety of subscription services that the customer can select based on its cyber security needs.

13. The cyber threat intelligence market is highly competitive. The competitive nature of the market is driven, in part, by the increase in cyber threats and the need for customers to employ proactive and complex security measures to protect the systems fundamental to their business operation. To do this, customers rely on their service providers, such as RedSense, to provide innovative, high-quality, accurate, and timely threat intelligence data. Failure to provide this high-quality, accurate, and timely data has significant consequences. For example, if RedSense provides a customer with threat intelligence data that incorrectly identifies a potential threat, a customer could spend resources to protect itself from a threat, only to realize they devoted resources to prevent against the wrong threat. Likewise, if RedSense's threat intelligence is untimely, a customer could have

already been attacked and would have to spend thousands of dollars to remediate something it could have prevented with timely threat intelligence.

14. For the same reason, customers in this market are highly attuned to the reputation of their service providers. A hint or even a rumor regarding impropriety, ethical concerns, or a similar vulnerability is enough to ruin the service provider's reputation and cause a customer to seek their threat intelligence services from another, more reputable source that they can trust. If that trust is broken in this industry, it is nearly impossible to repair the relationship. To that end, RedSense is also obligated by way of its customer service agreements to uphold strict operational security measures, perform under industry established and recognized standards, and that failure to do so is cause for breach and termination of said agreements—agreements that Bohuslavskiy has an intimate knowledge of.

15. RedSense has engaged significant efforts to be a threat intelligence service provider that its customers can rely on and trust. This includes, for example, entering into partner agreements with like-trusted industry leaders with strong reputations such as CISA (Cybersecurity and Infrastructure Security Agency, a division within the United States Department of Homeland Security) and other industry leaders, actively participating to support the FBI's cyber missions, and taking proactive measures to align itself with industry proven

standards such as SOC 2.[1] As a result of this effort, RedSense has developed a reputation of being reliable, trustworthy, and competent.

B. Bohuslavskiy's Involvement with RedSense

16. In December 2022, David Montanaro, a partner of RedSense and its current CEO, and Michael Zieger, a former partner of RedSense, connected with Bohuslavskiy, who they both knew from a prior employment at AdvIntel, regarding Bohuslavskiy potentially joining RedSense as a partner. At the time, Montanaro and Zieger believed that, given Bohuslavskiy's experience in the threat intelligence space and his ability to provide threat intelligence data, he would add value to the RedSense team.

17. On December 22, 2022, the then-existing RedSense Partners[2] voted unanimously to onboard Bohuslavskiy as a partner of RedSense. As a result of this decision to onboard Bohuslavskiy, the existing Partners and Bohuslavskiy executed the RedSense Restructuring & New Owner Onboarding Agreement

[1] SOC 2 is a cybersecurity compliance framework developed by the American Institute of Certified Public Accountants and is considered to be the industry gold standard for demonstrating commitment to protecting consumer data.

[2] At the time, the existing partners of RedSense were David Montanaro, Kevin Stear, Michael Zieger, and Bryan VanSickle.

("Onboarding Agreement")[3]. A true and accurate copy of the Onboarding Agreement as executed by Bohuslavskiy on January 25, 2023 is attached to this Complaint as **Exhibit A**.

18. Pursuant to the Onboarding Agreement, each partner of RedSense agreed to provide $100,000 in seed funding or, in the alternative, an "in-kind" contribution for the formation of RedSense. Ex. A, § 1.1. Bohuslavskiy specifically agreed to provide "'in kind funding' in the form of Threat Intelligence and Intellectual Property for Company benefit and use by the Company in lieu of the $100,000 seed funding contribution as part of this agreement with RedSense, LLC." *Id.* RedSense understood that the "in kind" funding that Bohuslavskiy was obligated to provide included but was not limited to AdvIntel[4] threat intelligence reports and historical adversary infrastructure intelligence along with the associated data sets, reports, and access data (collectively, "Obligated In-Kind Funding"). Providing the Obligated In-Kind Funding was a condition precedent for Bohuslavskiy joining RedSense as an equal partner of the LLC.

[3] "Partner," "Founder," and "Equal Owner" are used interchangeably within the Onboarding Agreement and have the same meaning.

[4] Bohuslavskiy, Zeiger, and Montanaro all worked at AdvIntel, and Bohuslavskiy was one of AdvIntel's co-founders. Prior to the founding of RedSense, AdvIntel ceased operations. As co-founder of AdvIntel, Bohuslavskiy represented to RedSense that he had ownership rights in certain intellectual property formerly belonging to AdvIntel.

19. As part of the Onboarding Agreement, Bohuslavskiy represented and warranted that he was not party to any other agreement that would restrict his ability to perform his obligations under the Onboarding Agreement (including his obligation to provide the Obligated In-Kind Funding). Ex. A, § 6.1. He also represented and warranted that "no third party can claim any rights to any intellectual property or other proprietary right possessed by that Founder as it relates to [RedSense]." *Id.* Given that RedSense anticipated incorporating the threat intelligence and intellectual property that Bohuslavskiy provided into the data it provides to its customers (indeed, the promise to provide such threat intelligence and intellectual property was a material term of the Onboarding Agreement and is the sole reason that Bohuslavskiy was asked to join RedSense), it was critical that no third party could assert any rights to the Obligated In-Kind Funding Bohuslavskiy provided.[5] Accordingly, the Onboarding Agreement required Bohuslavskiy to expressly agree and acknowledge that the representation and warranty applied to him and compliance with the terms of the representation

[5] If the threat intelligence or intellectual property Bohuslavskiy provided belonged to a third party, RedSense's use or incorporation of that threat intelligence data in deliverables to RedSense customers could constitute infringement. This would be ruinous to RedSense who would be precluded from further use of what Bohuslavskiy provided as his Obligated In-Kind Funding and would mean that what Bohuslavskiy provided had no value.

and warranty was an additional consideration for Bohuslavskiy joining RedSense as an equal partner. *Id.*

20. Bohuslavskiy executed the Onboarding Agreement on behalf of himself and Affix Advisory, LLC (a New Jersey LLC of which Bohuslavskiy is the sole member).

21. Pursuant to the Onboarding Agreement, the partners of RedSense expected that Bohuslavskiy would provide the required Obligated In-Kind Funding. And, at first, it appeared that Bohuslavskiy did provide this Obligated In-Kind Funding in the form of AdvIntel threat intelligence reports and historical adversary infrastructure intelligence along with the associated data sets, reports and access data because he and his team incorporated these reports, intelligence, and data into the deliverables that RedSense offered its customers. Throughout 2023, the intelligence reports RedSense delivered to its customers was consistent with and incorporate what the other partners understood constituted the Obligated In-Kind Funding. Notably, even during this time Bohuslavskiy maintained sole access to the Obligated In-Kind Funding. In reliance on the representation and warranty provided by Bohuslavskiy, the other partners of RedSense treated Bohuslavskiy as a partner of the LLC.

22. Additionally, because current RedSense partners had worked with Bohuslavskiy previously, at the outset, they did not have reason to distrust

Bohuslavskiy's promises when he stated that he would provide the Obligated In-Kind Funding and that he was in possession of it. It was only in mid-2024 when RedSense observed a significant drop-off in reporting that RedSense had reason to investigate Bohuslavskiy's promise. Subsequently, every attempt by RedSense partners to access the Obligated In-Kind Funding was rebuked.

C. Bohuslavskiy's Responsibilities as RedSense Chief Research Officer

23. As RedSense's Chief Research Officer, Bohuslavskiy was responsible for overseeing the day-to-day management of the threat research business function, budget, and resourcing. He led the RedSense Threat Intelligence Team. The Threat Intelligence Team is tasked with RedSense reporting, providing customer briefings, responding to requests for information from customers and potential customers, and participating in sales meetings. Additionally, Bohuslavskiy was responsible for managing and staffing the RedSense Engineering Team under his department.

24. To staff the engineering team, Bohuslavskiy onboarded three freelance engineers who were freelancers with EasyStaff. EasyStaff is a third-party service that allows companies to hire freelancers. In March 2023, RedSense and EasyStaff executed a services agreement, whereby RedSense would pay EasyStaff for the work performed by the freelancers.

25. Subsequently, Bohuslavskiy sought to hire his brother, Dmitriev, to serve as a strategic consultant to RedSense. Bohuslavskiy recommended to the other partners that RedSense should hire Dmitriev. It was anticipated that Dmitriev would be involved in strategic management, product development, team management, and other key product consulting roles, and would do these roles under the guidance and direction of Bohuslavskiy. Dmitriev joined RedSense as a strategic consultant on August 1, 2023.

D. Bohuslavskiy's Access to RedSense Confidential and Trade Secret Information

26. As part of Bohuslavskiy's role with RedSense, RedSense entrusted Bohuslavskiy with its existing and potential customer relationships and its confidential and trade secret information to use to fulfil his responsibilities to RedSense, maintain existing relationships, and bring in new business. Because the other partners of RedSense believed that Bohuslavskiy had provided the Obligated In-Kind Funding to join as a RedSense partner (which later turned out to be a false belief), RedSense treated Bohuslavskiy as a partner, which meant that he had access information that RedSense considers to be trade secret, including customer information and information about RedSense's offerings that were in development or had not been advertised to the public yet that RedSense leveraged to maintain a competitive advantage in the threat intelligence market. Specifically, RedSense

treats the following information as trade secret information ("RedSense Trade Secrets"):

a. REDACTED

b. REDACTED

c. REDACTED

d. REDACTED

e. REDACTED

f. REDACTED

REDACTED

27. The RedSense Trade Secrets derive independent economic value from not being generally known to, or readily ascertainable, by the public or to persons who can obtain value from their use. If these secrets were known to customers, they would not have to retain the services of RedSense. If known to competitors, they could replicate the threat intelligence and other services that RedSense provides to its customers without incurring the substantial development costs that RedSense incurred to develop its trade secret information, thereby defeating RedSense's market advantage.

28. Because these trade secrets are critical to its business, RedSense maintains the secrecy and confidentiality of this information and takes robust steps that align with standard industry practices to ensure that this information remains protected. For example, RedSense does not share this information absent a confidentiality agreement. This is true for both the customers that RedSense receive threat intelligence briefings and the employees or contractors that have access to the RedSense Trade Secrets to the extent necessary to perform their responsibilities. When RedSense shares these intelligence briefings with customers, it does so via secure electronic communication, encrypted means, and with confidentiality markings. Internally, RedSense maintains secure storage and

controls access of the secure storage only to those whose access is necessary for carrying out their responsibilities. Individuals and teams are given unique credentials and are prohibited from sharing them with others. When individuals leave RedSense, their access to the secure RedSense systems are immediately terminated to prevent unpermitted access to the RedSense Trade Secrets.

E. Bohuslavskiy Fails to Deliver Work Product That RedSense Paid For

29. On or around mid-2024 RedSense, it became apparent that although Bohuslavskiy was responsible for various teams and deliverables, there was a consistent failure to deliver work product as promised. All RedSense engineers who are responsible for writing code are obligated to check the source code into RedSense's GitHub repository. The purpose of this is to ensure that the code, which belongs to RedSense (and not to any one engineer), is accessible to the company and can be leveraged by RedSense as needed. This also ensures business continuity in the event an engineer or other staff leaves RedSense. This practice of checking the source code back into the GitHub repository is standard industry practice for companies that use GitHub to support their source code development. While the engineering staff that was *not* managed by Bohuslavskiy complied with this directive, the engineering team that was managed by Bohuslavskiy failed to upload completed source code to RedSense's GitHub repository. RedSense is informed and believes, and on that basis alleges, that the failure of Bohuslavskiy

and his team to upload the source code to GitHub is either because Bohuslavskiy's engineering team did not write the lines of code (and thus, there was nothing to upload) or that they did complete the coding tasks, but intentionally chose to ignore standard practice so that Bohuslavskiy and his team—that he solely managed—were the only ones that had access to this code. By doing this, RedSense is informed and believes, and on that basis alleges, Bohuslavskiy was in a position to abscond with the code that belonged to RedSense was in a position of leverage—if only Bohuslavskiy and his team could access the code, then Bohuslavskiy knew that he could extract what he wanted from RedSense.

30. An example of this failure to upload code that belonged to RedSense to the GitHub repository was with the AI-Driven Intel Search ("AIDIS") Solution, an automation tool that Bohuslavskiy and his team were responsible for developing under the internal code name Project Pylon. AIDIS would allow RedSense to deliver more targeted threat intelligence to its customers based on a more rapid AI-driven search and report generation capability. RedSense socialized the use of this tool with customers and referenced the tool in customer reports as something RedSense utilized to support its customer relationships. Based on feedback from customers, RedSense is informed and believes, and on that basis alleges, that this automation tool was a valuable tool for customers to use and something that differentiated RedSense from other threat intelligence companies. RedSense is

informed and believes, and on that basis alleges, that Bohuslavskiy also knew that this tool was a value-add for RedSense.

31. Not only was the source code related to AIDIS never uploaded to the GitHub repository, but Bohuslavskiy never delivered a single project roadmap nor produced a single deliverable related to the project. Other RedSense employees that were not part of Bohuslavskiy's team had to create and provide the project roadmap that Bohuslavskiy failed to deliver. The same thing happened with the Forum Scraping code project: Bohuslavskiy and his team were responsible for delivering this code, and no code was ever delivered (or possibly, even developed).

32. In January 2025, RedSense conducted an asset inventory of the assets that Bohuslavskiy and the team he managed were responsible for delivering. This inventory was conducted because of ongoing concerns that Bohuslavskiy was failing to deliver the promised deliverables, even though RedSense was making payments for these deliverables. The objective of the inventory was to reconcile the invoices that RedSense had received with the payments that had been made and the deliverables that had not been received.

33. The results of this asset inventory were shocking. Bohuslavskiy was specifically asked to provide the following assets and to identify where the assets were stored within the RedSense environment: all deliverables that the EasyStaff freelancers worked on, the threat intelligence and intellectual property that was

part of the Obligated In-Kind Funding that Bohuslavskiy was obligated to provide as a condition precedent for becoming a partner of RedSense, threat intelligence reports Bohuslavskiy was responsible for developing or sourcing, the AdvIntel reports, deliverables from Dmitriev that Bohuslavskiy oversaw, including product roadmap, project plan, estimates for hours and budgets, the Pyrus application (access, data, invoices), and an overall accounting for these assets. Bohuslavskiy declined to provide any of these assets. He also failed to provide information as to where any of these assets had been saved. This led the other partners of RedSense to conclude that either Bohuslavskiy was holding the assets hostage for leverage over the other partners, Bohuslavskiy had no intention of ever providing these assets, or no work had been done on any of these assets. In any event, this prompted RedSense to conduct a full-scale internal audit of all the money it had paid Bohuslavskiy and every member of his team.

F. RedSense Discovers Evidence of Improper Invoicing by Bohuslavskiy

34. As part of this audit, RedSense checked for the existence of the expected deliverables and supporting invoices for the monthly payments made to Dmitriev, because his Strategic Consultant agreement with RedSense states specific deliverables under the Product Development section (which RedSense contends is the core deliverable) and a specific annual salary paid in US Dollars with no other benefits provided (no bonus provision, no requirement for RedSense

to pay the salary in a currency other than US Dollars, and no obligation for RedSense to incur the cost of currency exchange fees). RedSense received invoices on Affix paper for the tasks and deliverables Dmitriev "completed," which Bohuslavskiy was responsible for approving. In every instance, the invoice was for more than the expected amount. Nevertheless, Bohuslavskiy approved payment after payment to Affix. Because Bohuslavskiy managed Dmitriev, RedSense is informed and believes, and on that basis alleges, that Bohuslavskiy knew that his brother had not performed the promised work and therefore, was not entitled to payment (beyond the annual compensation that RedSense is informed and believes, and on that basis alleges, that had already provided to Dmitriev under his agreement with RedSense[6]). Not only did the audit reveal that Bohuslavskiy approved payments for work that was never completed (that Bohuslavskiy knew was never completed because he managed these projects), Bohuslavskiy also approved payments for invoices for more than what he was entitled to under Dmitriev's agreement with RedSense, including for example, payments that appeared to be unapproved bonuses, payments in non-US Dollar currencies, and payments covering currency exchange rate—none of which RedSense had agreed

[6] Because Dmitriev's payments were paid directly to Affix (Bohuslavskiy's LLC) it is possible that Bohuslavskiy never made a subsequent payment to Dmitriev and instead kept the money for himself. Therefore, only Bohuslavskiy would know if *he* (via Affix) properly paid Dmitriev.

to pay. It was bad enough that RedSense had made payments for work that was not competed; it was even worse that Dmitriev was paid more for this non-existent work—from RedSense's perspective, any payment it has made to Dmitriev/Affix on behalf of Dmitriev represent an overpayment because RedSense has not received the deliverables it paid for.

35. For tax purposes, Bohuslavskiy had requested that RedSense make payments to him via his LLC, Affix. Accordingly, Affix would invoice RedSense for the amount that Bohuslavskiy was due, Bohuslavskiy would approve the payment, and then Affix (Bohuslavskiy) would get paid. An audit of these invoices revealed thousands of dollars in payments in excess of what Bohuslavskiy was owed, all of which Bohuslavskiy had approved—either directly or tacitly—for himself. RedSense is informed and believes, and on that basis alleges, Bohuslavskiy knew he was not entitled to this extra payment when he approved the Affix invoices and approved these invoices for the sole purpose of defrauding RedSense into making payments to Bohuslavskiy.

36. The same was true when RedSense investigated the payments made to the EasyStaff freelancers. Payment records demonstrate that RedSense paid over $400,000 USD to the freelancers for tasks such as threat research and intelligence that *to date, RedSense has never received*. RedSense is informed and believes, and on that basis alleges, that Bohuslavskiy approved each of these EasyStaff invoices

even though he had knowledge that the deliverable had not been provided to RedSense. Because EasyStaff is a freelance agency, RedSense understands that once a payment is made to EasyStaff, it is distributed to the freelancers based on time entries and task assignments in the portal. When RedSense contacted EasyStaff, RedSense discovered that there were no time entries or task assignments, indicating no work had been performed by these freelancers for RedSense.

37. This led RedSense to understand that the freelancers retained by Bohuslavskiy did not perform that work that RedSense paid thousands of dollars for. RedSense is informed and believes, and on that basis alleges, that Bohuslavskiy may have even used the EasyStaff freelancers as a way to funnel money to himself in a covert way. Specifically, RedSense is informed and believes, and on that basis alleges, that Bohuslavskiy and the freelancers (to the extent they even exist) colluded together such that the payment for their nonexistent work would be paid to the freelancers, who would then "return" the payment to Bohuslavskiy.

38. Pyrus is a third-party hosted software application that includes accounts payable, knowledge base, service desk, and workflow management tools. At the request of Bohuslavskiy, RedSense paid for software license to the Pyrus application so that Bohuslavskiy and his team would have access to the Pyrus

application. The idea was that Bohuslavskiy and his team would use the Pyrus application to track and manage the deliverables owed to RedSense. To pay for the software licenses (for the software that Bohuslavskiy and his team used for the work supposedly performed), Affix (Bohuslavskiy) invoiced RedSense, who would then in turn distribute payments to Affix for the expense, who supposedly used the money to pay Pyrus. When RedSense attempted to investigate the invoices and deliverables to reconcile the difference in the expenses compared to the software license fees, RedSense was blocked from doing so. Because the invoicing had been done by Affix (Bohuslavskiy), Bohuslavskiy was listed as the account administrator. When Bohuslavskiy resigned from RedSense in February 2025, he took steps to lock RedSense out of the Pyrus application. Pyrus confirmed to RedSense that no one at RedSense had access to this work product. Therefore, it is unclear if Pyrus actually got paid by Affix, if Bohuslavskiy and his team actually used Pyrus to complete their assigned work, or if the Pyrus software licenses were simply a phony expense. In any event, RedSense paid for the software license and deliverables and did not receive any work product. During the same time, Bohuslavskiy began cutting key RedSense employees out of meetings with key customers. Based on the events that transpired after Bohuslavskiy's resignation, RedSense is informed and believes, and on that basis alleges, that this was done intentionally in preparation for Bohuslavskiy's

interference with RedSense customers, because he wanted to push RedSense out of the picture so that he was in position to better usurp the relationships.

G. Bohuslavskiy Refuses to Participate in the Operation of RedSense, Disclaims His Duties, and Resigns.

39. By January 2025, RedSense had spent thousands of dollars on threat intelligence, reports, and source code, yet had no work product to show for it. Additionally, unbeknownst to RedSense partners at the time, Bohuslavskiy was responsible for approving invoices, including duplicate invoices (multiple invoices for the same amount for the same services within the same month), for work that was seemingly never performed. All the while, RedSense had ongoing obligations to its customers to provide high-quality, reliable, timely, and accurate threat intelligence. To satisfy these obligations, RedSense had to expend additional funds to source these assets from elsewhere, given that none of the assets Bohuslavskiy was responsible for had materialized.

40. RedSense convened a special partner meeting on February 6, 2025 to discuss the immediate financial needs of RedSense and discuss the steps the partners would take both near and long term to protect RedSense and to ensure the business could benefit from expansion and growth opportunities. At the time, because the other RedSense partners believed that the threat intelligence and intellectual property that Bohuslavskiy provided to RedSense as his Obligated In-Kind Funding had been properly conveyed to RedSense, and because they relied

on the representations of Bohuslavskiy to this effect, the other partners viewed Bohuslavskiy as a partner of RedSense. Accordingly, he was provided notice of the special partner meeting. Bohuslavskiy, however, chose not to attend. Bohuslavskiy's lack of participation was not particularly surprising given that on January 23, 2025, Bohuslavskiy sent an email to partners and non-partners self-suspending any duties he had to RedSense.

41. While the other, then-current partners of RedSense (Montanaro, Stear, VanSickle) executed an agreement regarding the steps to take to protect RedSense finances, Bohuslavskiy refused. This again was consistent with the emails he was sending to both the other RedSense partners and nonpartners where he was disclaiming his duties to RedSense.

42. During this time, RedSense was also making preparations to become compliant with SOC 2. As part of these preparations, RedSense revamped and instituted a companywide security program that required all partners, staff, and third-party vendors to executed various documents including a Confidential Information and Invention Assignment Agreement, commonly referred to as a "CIIAA."

43. On February 18, 2025, Montanaro sent Bohuslavskiy an email, requesting that he sign the CIIAA. Given that the assets that Bohuslavskiy was responsible for and were not accounted for during the asset inventory, RedSense

needed confirmation that the assets existed and that there was no dispute that the assets belonged to RedSense.

44. Not only did Bohuslavskiy refuse to sign the CIIAA, but he also actively sent messages via the Signal messaging application to other individuals including the entire RedSense staff, Dmitriev, and the EasyStaff freelancers encouraging them to not sign. He claimed that EasyStaff freelancers were owed outstanding payments and will not sign the CIIAA until paid. Of course, the subsequent invoice reconciliation revealed that EasyStaff was paid and overpaid—because RedSense still has not received the deliverables, RedSense believes that *any* payment to EasyStaff constitutes an overpayment.

45. On February 24, 2025 at 3:34 p.m., Montanaro informed Bohuslavskiy that he had made a good faith payment to EasyStaff to encourage the signing of the CIIAA. As the subsequent invoice reconciliation revealed, the good faith payment was an *overpayment*, and not something that was outstanding and as confirmed by EasyStaff, no work products or work location references existed in any of the completed and accepted tasks since inception.

46. Approximately one hour later, at 4:49 p.m., Bohuslavskiy submitted a resignation on behalf of himself and Dmitriev.

47. Simultaneous to Bohuslavskiy's resignation, RedSense became aware of a cyber incident that occurred on the evening of February 23, 2025 whereby the

RedSense systems used by Bohuslavskiy and his team were accessed, and any existing source code was copied out, and the file system was destroyed. RedSense's investigation into the incident revealed the credentials used to access the systems were those used by Dmitriev, Bohuslavskiy's brother and a RedSense Strategic Consultant. Given the timing and the use of Dmitriev's credentials, RedSense is informed and believes, and on that basis alleges, that this theft of RedSense property was done by or at the direction, request, or encouragement of Bohuslavskiy. RedSense is informed and believes, and on that basis alleges, that Bohuslavskiy's erratic conduct was a result of RedSense finally discovering Bohuslavskiy's misconduct and a desire to punish the remaining partners of RedSense in retaliation for the steps RedSense had taken.

48. The next day following his resignation, Bohuslavskiy threatened to go public with his grievances against RedSense, including "informing each customer" of what he perceived to be "illegal action" on the part of RedSense (the requiring of its partners, staff, and vendors to execute CIIAA to formalize the assignment of the assets RedSense already owned).

49. As a result of Bohuslavskiy's threats, RedSense's corporate counsel issued a cease-and-desist letter to Bohuslavskiy demanding that he cease and desist communications with RedSense customers, partners, employees, and contractors. A true and accurate copy of the cease-and-desist letter dated February 25, 2025 is

attached to this Complaint as **Exhibit B**. The letter specifically informed Bohuslavskiy that his threats to contact RedSense customers and disparage RedSense would irreparably harm the operations and business reputation of RedSense.

H. Bohuslavskiy Launches Smear Campaign Repeatedly Disparaging RedSense to Its Existing and Prospective Customers.

50. Bohuslavskiy made good on his threat to disparage RedSense customers and smear the reputation of RedSense. He began a campaign of contacting RedSense customers, disparaging RedSense, claiming he had "ethical concerns" about the company, insinuating that RedSense cannot adequately service the customer relationship, and advertising his own threat intelligence offerings, and encouraging customers to contact Bohuslavskiy directly to ensure "seamless intel provision and continuity."

51. For example, beginning on March 6, 2025, Bohuslavskiy contacted at least a dozen RedSense customers, including REDACTED [redacted] REDACTED RedSense presently has no reason to believe that no less than all customers have been contacted repeatedly. A true and accurate copy of the customer emails that were forwarded to RedSense are

attached to this Complaint as **Exhibit C**.[7] In these emails, he informed the customers of vague "ethical concerns" he had about RedSense, provided threat intelligence reports that were created by his team (and not RedSense) and encouraged the customers to contact him directly via phone, Signal, or email if the customer desired to engage his services. RedSense became aware of these emails when the customers forwarded the emails or reached out to RedSense, expressing concern and confusion about these emails, and raising questions as to whether RedSense and/or Bohuslavskiy had been compromised.

52. Also on March 6, Bohuslavskiy published a post to his public LinkedIn page regarding his resignation. *See* Figure 1. As with his customer emails, Bohuslavskiy explicitly complained of his ethical concerns regarding RedSense.

[7] A compendium containing the true and accurate copies of the customer emails Bohuslavskiy sent following his resignation is attached to this Complaint as **Exhibit C**.

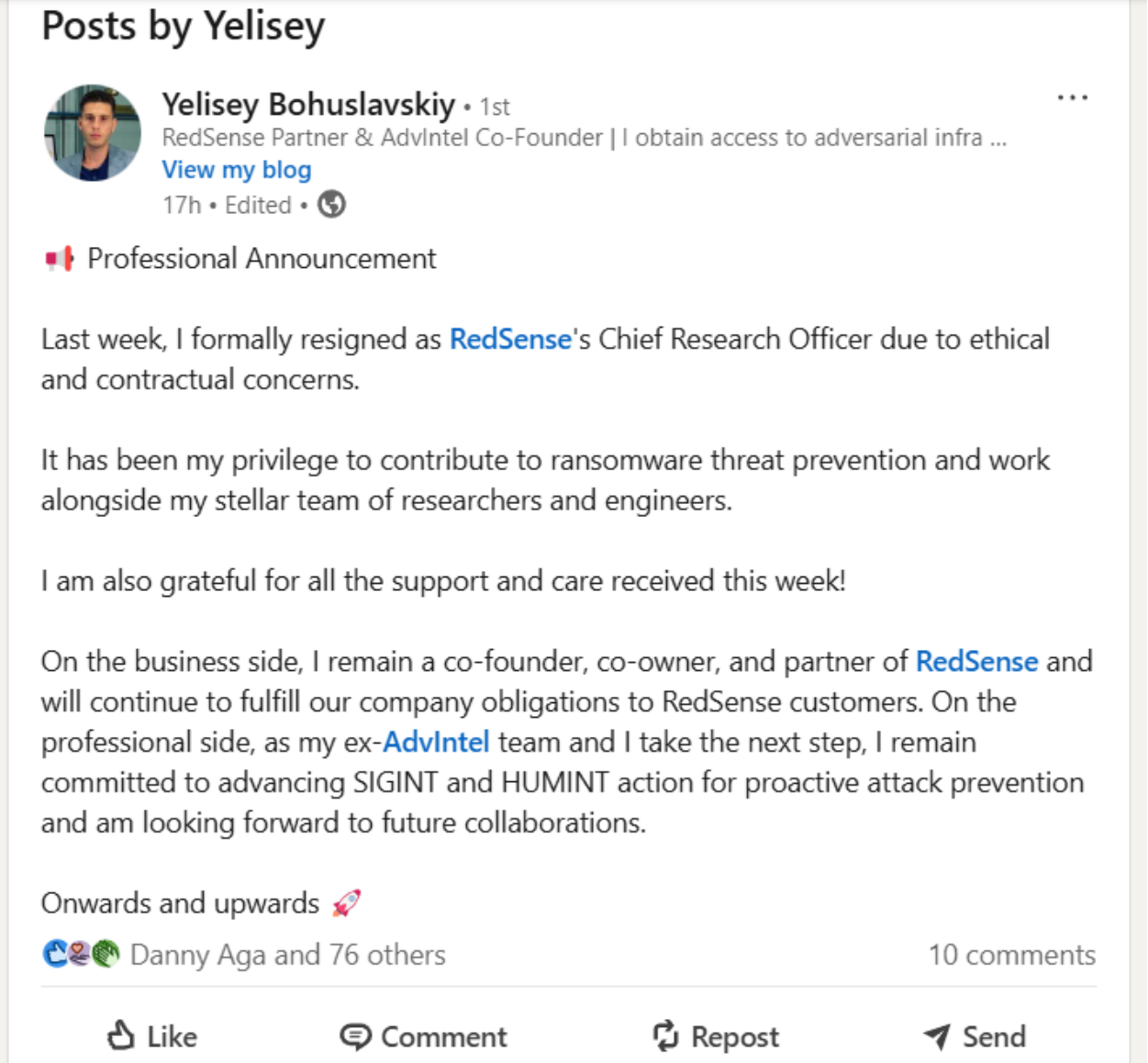

Figure 1, Bohuslavskiy LinkedIn Post, dated March 6, 2025[8]

[8] Yelisey Bohuslavskiy, *Professional Announcement*, LinkedIn (Mar. 6, 2025, (9:10 p.m. UTC), available at https://www.linkedin.com/posts/yelisey-bohuslavskiy-214a02bb_professional-announcement-last-week-activity-7303522308663435264-fyIj?utm_source=share&utm_medium=member_desktop&rcm=ACoAABl_jQ8Br3x-Nm5Cf1p2git35cVBYjV764U (last accessed Jun. 25, 2025).

53. On March 17, 2025, RedSense's outside counsel, Crowell & Moring LLP ("Crowell"), sent Bohuslavskiy a further cease and desist letter demanding that he stop all communications with RedSense customers immediately. A true and accurate copy of this letter is attached to this Complaint as **Exhibit D**. The cease-and-desist letter did not deter Bohuslavskiy. Indeed, it emboldened him.

54. On March 17 and 18, Bohuslavskiy reached out to REDACTED and potentially other customers, with an update regarding upcoming ransomware attacks targeting healthcare companies. *See* Ex. C. Like with the prior emails, Bohuslavskiy encouraged the customer to contact him and his team directly, claiming that his team and not RedSense could protect the customer's interests.

55. On April 29, 2025, Bohuslavskiy emailed REDACTED and potentially other customers, with a request to meet for a Q1 intelligence briefing, which he claims that RedSense failed to deliver. *See* Ex. C. RedSense is informed and believes, and on that basis alleges, that Bohuslavskiy made these claims so that the customer would erroneously believe that RedSense was not honoring its contractual obligations to REDACTED This, of course, would make REDACTED less likely to continue its relationship with RedSense or, at minimum, cause REDACTED to have concerns about the viability of RedSense as its provider of threat intelligence. Bohuslavskiy also emphasized that the intelligence his team will present relies upon his "unique" access to adversarial sources, and that he was not offering to

deliver publicly available, open-source, or recycled intelligence. Once again, Bohuslavskiy instructed the customer to come to him with any questions.

56. Bohuslavskiy's conduct with respect to his customer outreach has not been in the best interest of RedSense or its customers. Specifically, customers have reached out to RedSense with confusion and concern. Because Bohuslavskiy sent these communications via a *personal Gmail* email address and included a statement that he resigned from RedSense, customers have asked whether the email is legitimate (because they expect RedSense communications to come via a RedSense email address), whether it is a scam, whether the email is a phishing lure, or whether the email is actually coming from Bohuslavskiy or if someone is impersonating Bohuslavskiy. Based on communications with customers, RedSense is informed and believes, and on that basis alleges, that customers who expect to receive correspondence regarding the RedSense services via official RedSense channels are confused when communications come from personal email addresses and do not understand why they are coming from an individual who has stated in the outreach that he has resigned from RedSense. RedSense is informed and believes, and on that basis alleges, that customers, who are unfamiliar with the corporate structure of RedSense, are left wondering whether Bohuslavskiy is speaking on behalf of RedSense and whether he is authorized to do so. This is further compounded by Bohuslavskiy offering to provide continued threat

intelligence through Affix (Bohuslavskiy's LLC), which RedSense is informed and believes, and on that basis alleges, that would be an unknown and unfamiliar entity to RedSense's customers.

57. Based on communications RedSense has had with its current customers, RedSense is informed and believes, and on that basis alleges, that Bohuslavskiy is actively communicating with RedSense customers to date, despite multiple demands that he cease this damaging conduct immediately. Based on communications with its customers, RedSense is informed and believes, and on that basis alleges, that the customers have had to spend considerable time and resources dealing with Bohuslavskiy's emails because they have had to spend time to determine if Bohuslavskiy's emails are a scam, if RedSense can service the relationship, and whether the customer would be better served by Bohuslavskiy's team.

58. Additionally, because of the nature of the threat intelligence industry, RedSense is informed and believes, and on that basis alleges, that an insinuation that there are "ethical concerns" surrounding RedSense would be enough to permanently damage RedSense's reputation within this market. Because of these increased sensitivities when dealing with cybersecurity protection, regardless of what the "ethical concern" is or whether there is any merit to it (there is not), such

insinuations may lead a customer to believe that it can no longer entrust RedSense to service the relationship without compromise.

I. RedSense Attempts to Resolve Dispute Amicably with Bohuslavskiy; Bohuslavskiy Refuses.

59. On March 17, Crowell sent Bohuslavskiy a cease and desist letter demanding the return of the RedSense property that RedSense's investigation revealed Bohuslavskiy had never provided to RedSense: (1) AIDIS (Project Pylon) including all software and documentation; (2) Pyrus platform including all data since inception; (3) EasyStaff Deliverables, including code, data, research, LLM, documentation; (4) Igor Dmitriev's deliverables as stated in the agreement dated August 1, 2023; (5) Forum Scraping code and results to date; (6) OpenCTI instance and all RedSense Threat Intelligence contained therein; and (7) All AdvIntel Reports and threat intelligence since inception. *See* Ex. D at 2. This was either property that RedSense had directly paid for, or, in the case of the AdvIntel reports and threat intelligence, constituted the Obligated In-Kind Funding that Bohuslavskiy was obligated to provide in consideration of him becoming an equal partner of RedSense and that he had represented and warranted that he had the ability to provide.

60. Bohuslavskiy's response was concerning. A true and accurate copy of Bohuslavskiy's response, dated March 31, 2025, is attached as to this Complaint as **Exhibit E**.[9] In response to RedSense's demand that he return to RedSense the assets and intellectual property that RedSense owns, he made the shocking admission that he believed the transfer of such property would be "improper and legally unsound" because "RedSense definitely has no claim to this IP and any such transfer — if it were even possible — would violate binding agreements," including expressly that it would violate binding agreements with Advanced Intelligence ("AdvIntel"). Ex. E at 2. Bohuslavskiy also expressly stated that "RedSense clearly has no legal entitlement" to the AdvIntel reports. *Id.* at 6.

61. Bohuslavskiy has no basis to claim that it was "unsound" for RedSense to demand the property it had paid for. Indeed, Bohuslavskiy knew that he had no basis to refuse, given that he was the person responsible for approving the payments *from* RedSense for this very property. But even more concerning was his admission that the transfer of the AdvIntel threat intelligence and reports "would violate binding agreements"

[9] In his March 31 response, Bohuslavskiy focused more on launching personal attacks against Crowell & Moring LLP ("Crowell") and Ms. Chakrabarti (counsel of record for RedSense) and questioning the validity of Crowell's representation of RedSense, rather than on focusing the merits of the letter.

62. In 2023, when Bohuslavskiy executed the Onboarding Agreement, his joining RedSense as an equal partner was conditioned on two things: (1) the provision of Obligated In-Kind Funding in the form of intellectual property and threat intelligence, which the other RedSense partners understood to include AdvIntel threat intelligence reports and historical adversary infrastructure intelligence along with the associated data sets, reports and access data; and (2) representing and warranting that he was not party to any other agreement that would restrict his ability to perform his obligations under the Onboarding Agreement (including his obligation to provide the Obligated In-Kind Funding). This admission from Bohuslavskiy contradicted both of these promises: he admitted that this Obligated In-Kind Funding *had never been provided to RedSense at all* and that Bohuslavskiy *had no right to promise these reports*. In short, Bohuslavskiy revealed that he never fulfilled the condition precedent that was required for him to join RedSense as an equal partner. Given this shocking admission, the other partners of RedSense realized that although they had been treating Bohuslavskiy as an equal partner of RedSense, he actually was in violation of the Onboarding Agreement and that with respect to Bohuslavskiy, there was a lack of consideration supporting the Onboarding Agreement. Accordingly, there were now serious questions as to whether Bohuslavskiy was ever a proper partner. Indeed, given the other misconduct of Bohuslavskiy that RedSense had uncovered

since his resignation, RedSense had concerns that not only did Bohuslavskiy not possess the rights to the AdvIntel threat intelligence and reports, but he knew he did not possess the rights, never intended to convey the threat intelligence and reports to RedSense, and fraudulently made the representations and warranties contained in the Onboarding Agreement.

63. Over the next two months, RedSense tried to amicably resolve the outstanding issues with Bohuslavskiy. Yet Bohuslavskiy was never interested in addressing the substantive concerns raised by RedSense. He instead was more interested in blocking any meaningful discussion. For example, in nearly all of his communications, he has questioned the validity of Crowell's representation of RedSense and seeks privileged attorney-client communications between RedSense and Crowell to "prove" the propriety of the representation. *See generally* Ex. F.[10] Additionally, Bohuslavskiy has placed unreasonable and unrealistic demands on RedSense, including the demand that RedSense withdraw all its allegations it has asserted against Bohuslavskiy (as alleged in the March 17 cease and desist letter, Ex. C), the demand that RedSense unequivocally recognize his status as a legal partner of RedSense (despite serious doubts existing about his status as a partner given his admission that he never provided the Obligated In-Kind Funding that was

[10] A true and accurate copy of correspondence between Bohuslavskiy and Crowell from April – June 2025 is attached to this Complaint as **Exhibit F**.

required to join as a partner, Ex. E), and the demand for immediate restoration of his, Dmitriev's, and EasyStaff freelancers' access to the RedSense systems, even though Bohuslavskiy had submitted resignations for each of them, effective February 24, 2025 and even though RedSense had good reason to believe that Bohuslavskiy or Dmitriev or someone acting at Bohuslavskiy's direction was responsible for stealing RedSense code and destroying the file system where the code was stolen from. *See* Ex. F at 8 – 9.

64. During this time, Bohuslavskiy sent a letter directly to RedSense's CEO, David Montanaro, on April 14, 2025. A true and correct copy of this letter is attached to this Complaint as **Exhibit G**. In this letter he demanded restoration of access to the RedSense systems (which he was not entitled to following his resignation) and additional payments to the EasyStaff freelancers (which was improper because EasyStaff had already been compensated for work they either never performed or that was not delivered to RedSense as it was contracted for).

65. The most concerning part of this letter was what could only be interpreted as a veiled cyber threat by Bohuslavskiy against RedSense in retaliation to RedSense taking steps to protect the company and its rights. In connection with his contention that the EasyStaff freelancers were improperly terminated (even though Bohuslavskiy was the one who submitted a resignation on behalf of EasyStaff), Bohuslavskiy stated:

> In this case, the engineers who were terminated reside in a foreign jurisdiction, retain detailed knowledge of RedSense's internal systems, and operate within a global digital environment where anonymous and unregulated forums are known to exist. While I make no allegation of intent or misconduct on their part, it is well-documented within the cybersecurity industry that poorly managed terminations can lead to reputational, legal, and technical vulnerabilities — including the "leak" publication of company data on platforms such as XSS or BreachForums by disgruntled personnel claimed under a "company breached" banner. This is not a suggestion that any individual involved would act improperly, but an industry-known risk that must be treated with diligence.

Ex. G at 5. There is no other plausible explanation other than that this message insinuated a cyberattack against RedSense was imminent unless RedSense caved to Bohuslavskiy's demand. Given Bohuslavskiy's and the freelancers' knowledge of RedSense code system and their skillset in the cybersecurity space, RedSense is informed and believes, and on that basis alleges, that Bohuslavskiy and the freelancers have the skill and capability to carry out such a cyberattack as threatened.

66. During this time where Bohuslavskiy refused to engage meaningfully in a potential amicable resolution, made unreasonable demands, and threatened RedSense, he continued to communicate with RedSense's customers, denigrating the services RedSense provided and encouraging the customers to obtain their threat intelligence from Bohuslavskiy and his team directly. Although RedSense attempted to reach resolution of this dispute amicably and without court

intervention, Bohuslavskiy's responses demonstrated that he did not take the issue seriously and would not halt absent court intervention.

CLAIMS FOR RELIEF

FIRST CAUSE OF ACTION – FALSE ADVERTISING IN VIOLATION OF THE LANHAM ACT (15 U.S.C. § 1125)

67. RedSense repeats, realleges and incorporates by references paragraphs 1 through 66 as if set forth herein.

68. In his March 6, 2025 LinkedIn post, Bohuslavskiy publicly indicated that he was departing from RedSense due to supposed ethical issues, casting a negative light on the company. He also claimed that he would continue to provide cybersecurity services to RedSense customers as contracted, attempting to obfuscate the distinction between customers' relationship with RedSense and their relationship with him.

69. Beginning on March 6, 2025 and continuing to date, Bohuslavskiy has engaged in a rampant campaign of disparaging RedSense to its existing and potential customers, all the while peddling his own threat intelligence services, encouraging RedSense customers to forego their relationship with RedSense and obtain threat intelligence services directly through Bohuslavskiy. In these communications he insisted that only he could service the needs of the customers and that RedSense was ill-equipped to manage the relationship. In these communications he made multiple references to his continued affiliation with

RedSense but provided his personal contact information and encouraged customers to contact him directly.

70. In doing so, Bohuslavskiy leveraged the existing customer relationship with RedSense (RedSense is informed and believes, and on that basis alleges, that Bohuslavskiy used the RedSense name as a way to lend credibility to these communications) while advertising his personal ability to meet customers' needs and fulfil RedSense's contractual duties (insinuating that RedSense *could not* fulfil these duties), ultimately associating his name and services with the company from which he had already resigned, deceiving RedSense's customer base as to Bohuslavskiy's role within RedSense, his ability to speak on behalf of RedSense, and creating customer confusion as to who (RedSense or Bohuslavskiy) was the responsible party for servicing the customer account.

71. In his emails to RedSense customers, Bohuslavskiy implied that the quality of the cybersecurity monitoring he and his team could provide surpassed the capabilities of other vendors, implying RedSense lacked his team's "unique" access. He also impugned the reliability of RedSense's services: in his April 29, 2025 email(s), Bohuslavskiy misrepresented to at least one customer that RedSense failed to meet its customary obligations to the customer by failing to present a Q1 intelligence briefing. He then offered to arrange a time for the customer to meet with him instead of for an intelligence briefing.

72. After repeatedly charging RedSense with incapacity and misconduct so severe as to influence customers' business decisions, Bohuslavskiy promoted his services—not just as an alternative, but as a "seamless" continuation of the customers' existing relationships with RedSense. In doing this, Bohuslavskiy actively materially deceived customers to divert business from RedSense to himself.

73. By making a public LinkedIn post and solicitating business from a broad sample of RedSense customers, Bohuslavskiy's misrepresentations were aimed at the purchasing public of cybersecurity coverage.

74. The advertised services, which include providing threat intelligence and cybersecurity services to companies throughout the United States involves interstate commerce.

75. Bohuslavskiy's use of false or misleading representations of fact in commercial advertising to current and future customers of RedSense misrepresent the nature, characteristics, or qualities of RedSense's threat intelligence services.

76. Bohuslavskiy's use of false or misleading representation of fact has the tendency to deceive a substantial portion of the target consumer audience or actually deceives the target consumers.

77. Bohuslavskiy's false or misleading representations of fact are material because they are likely to influence the purchasing decision of target customers,

specifically current customers of RedSense who are determining whether RedSense will adequately service their cybersecurity and threat intelligence needs as well as prospective customers who are evaluating whether RedSense can be entrusted to protect their cybersecurity needs.

78. Because of Bohuslavskiy's false or misleading commercial statements, RedSense has suffered and will continue to suffer substantial harm to its customer relationships, including potentially diverted business to Bohuslavskiy, decreased customer loyalty and trust, and irreparable harm to the reputation of RedSense, which in an industry as sensitive and competitive as the cybersecurity industry would cause devastation to RedSense's ability to preserve its customer relationships and engage prospective customers.

SECOND CAUSE OF ACTION – TORTIOUS INTERFERENCE WITH CONTRACT

79. RedSense repeats, realleges and incorporates by references paragraphs 1 through 78 as if set forth herein.

80. RedSense maintains contractual relationships with all of its customers, including but not limited to: **REDACTED**

REDACTED In each of these instances, RedSense contracted to provide cybersecurity threat monitoring and reporting services to customers.

81. Prior to resigning from RedSense, Bohuslavskiy sent an email addressed to "RedSense Partners" where he aired various grievances against Stear. In addition to emailing the RedSense partners (Montanaro, Stear, VanSickle), he also included other RedSense staff. But most concerning is that Bohuslavskiy included a primary point of contact of customer REDACTED in the "TO" line of the email. The point of contact is not a partner of RedSense, he is not an employee of RedSense, and he is not a contractor or staff member of RedSense. Instead, the point of contact has a background as a digital forensic specialist and serves as Senior Principal at RedSense customer REDACTED as well as the primary the point of contact for the RedSense-REDACTED relationship.

82. RedSense is informed and believes, and on that basis alleges, that the inclusion of the point of contact was not accidental, but that Bohuslavskiy intentionally included the point of contact on the email airing out his internal dispute with RedSense so that REDACTED (and specifically, someone integral to RedSense-REDACTED relationship) would become aware of this dispute. The only reason for Bohuslavskiy to do that is to sow doubt in the mind of REDACTED.

83. When he resigned from RedSense, Bohuslavskiy threatened to go to all of RedSense customers. Based on conversations with customers and taking

Bohuslavskiy at face value, RedSense is informed and believes, and on that basis alleges, that Bohuslavskiy has contacted most, if not all, of RedSense's current customers.

84. Through his email campaign to, and conversations with, RedSense customers, Bohuslavskiy interfered with the relationship between RedSense and its customers by sowing confusion and doubt, falsely claiming RedSense has failed to meet its obligations, and arguing that his services were superior to those offered by other vendors, implicitly denigrating RedSense and the services it provides. In his April 29, 2025 email, Bohuslavskiy specifically claimed that RedSense failed to provide at least one customer with a customary Q1 intelligence briefing. RedSense is informed and believes, and on that basis alleges, that based on Bohuslavskiy's correspondence with the other partners of RedSense, his sole purpose in contacting the customers was to ruin RedSense's customer relationships in retribution for his grievances with RedSense. He sent multiple emails soliciting customers to consult with him directly, inducing them to breach their contracts with RedSense. He actively took steps to undermine the trust that these customers had in RedSense and urged customers to retain his services instead.

85. As the former Chief Research Officer of RedSense, Bohuslavskiy was intimately familiar with the existence and contents of RedSense's contracts with its customers, including which customers RedSense considered its top customers and

the individualized services RedSense provides for each customer. It is of no surprise that Bohuslavskiy has targeted RedSense's largest customers in his smear campaign. Furthermore, prior to his resignation and at the time when RedSense believed he was an equal partner of the LLC, Bohuslavskiy received sensitive information regarding RedSense's financial plans. Accordingly, he knew that interfering with the relationships RedSense has with its key customers would cause the most harm to RedSense.

86. By denigrating RedSense's offerings as a cybersecurity provider, Bohuslavskiy understood his interference would likely undermine RedSense's existing business relationships.

87. As a result of Bohuslavskiy's interference, RedSense's customers perceive RedSense as having failed to protect them from malicious and unwanted contact from Bohuslavskiy, causing the customers to lose the sense of security curated by RedSense's prior performance of the parties' contracts. Multiple customers contacted RedSense in confusion or alarm about Bohuslavskiy's missives, questioning whether they might be fraudulent phishing attempts. This question from customers implies that RedSense itself was compromised, and it was — not by hackers, but by someone misrepresenting his ongoing affiliation with RedSense.

88. Based on customer communications, RedSense is informed and believes, and on that basis alleges, that its customers have had to spend considerable time, effort, and resources to deal with these unwanted communications. Customers, such as but not limited to REDACTED [redacted] who have otherwise been happy with the services that RedSense has provided, have informed RedSense this ongoing issue with Bohuslavskiy has caused a dark stain on RedSense's reputation and has undermined the otherwise high quality of services customers had come to expect from RedSense. In many instances the Chief Information Security Officers ("CISO") of RedSense's customers have expressed their concern or otherwise uneasiness. RedSense is informed and believes, and on that basis alleges, that with respect to customers in the cybersecurity or threat intelligence space, it is the CISO who determines which service providers will be retained for threat intelligence. Therefore, the uneasiness of a CISO regarding a continued relationship with RedSense will likely result in that customer refusing to renew its contract or renegotiating it at a lower rate.

89. In at least one instance, REDACTED which is RedSense's largest customer, has recently expressed disappointment regarding the issues between Bohuslavskiy and RedSense. REDACTED has also become noticeably less engaged and responsive to RedSense and has yet to pay RedSense the outstanding amounts that are past due under the subscription contract REDACTED has with RedSense.

90. RedSense is informed and believes, and on that basis alleges that Bohuslavskiy has been actively communicating with key stakeholders at REDACTED for the purpose of denigrating RedSense and seeking to steal the business from RedSense. Based on the timing of Bohuslavskiy's resignation and email smear campaign, his escalations as a result of RedSense's attempts to resolve the issue amicably, and the timing of REDACTED first stopped payment of the amounts due under the contract with RedSense, RedSense is informed and believes that this is all a direct result of Bohuslavskiy's actions.

91. Prior to Bohuslavskiy's smear campaign, RedSense leadership and REDACTED leadership routinely were in communication and continuing to discuss ways to enhance the partnership and increase the quality of the services RedSense provided, or the value that REDACTED obtained from RedSense. Recently, however, REDACTED (prior to them becoming less engaged and responsive) has raised questions about the quality of the services and the value-add RedSense can provide. Specifically, they have requested that RedSense provide the AIDIS Solution automation tool

that Bohuslavskiy previously previewed to REDACTED. The problem, however, is that Bohuslavskiy has absconded with the AIDIS code and refuses to return it to RedSense.

92. Because Bohuslavskiy knows that RedSense does not have the AIDIS code (because he has refused RedSense's demand for its return), RedSense is informed and believes, and on that basis alleges, that Bohuslavskiy is holding hostage and leveraging the AIDIS Solution's functionality and capabilities in his conversations with Red Sens customers to cause them to doubt RedSense's capabilities and value.

93. **REDACTED** is another customer of RedSense. Retaining this customer is strategically important for RedSense, as this customer operates within RedSense's largest vertical—customers within the healthcare industry represent RedSense's largest market and largest potential customer base. By virtue of his involvement with RedSense, Bohuslavskiy would know of the strategic importance of the relationship with **REDACTED** Following Bohuslavskiy's contacting of key stakeholders at **REDACTED** and disparaging RedSense, the Director of Cyber Intelligence and Threat Engineering at **REDACTED** has instructed RedSense that it needs to "work it out with Bohuslavskiy." Like with **REDACTED** also received a preview of AIDIS and has requested that RedSense provide the AIDIS tool immediately. RedSense is informed and believes, and on that basis alleges, that

the demand to "work it out" is a result of REDACTED wanting access to AIDIS and the strain that Bohuslavskiy has placed on the RedSense-REDACTED relationship. Bohuslavskiy's actions have put RedSense in a position where it cannot provide this tool, because Bohuslavskiy stole the tool and refuses to return it to RedSense. RedSense is informed and believes, and on that basis alleges, that because Bohuslavskiy is aware of the strategic importance of the REDACTED customer relationship, Bohuslavskiy has incentive to market AIDIS capabilities as a selling point as to why customers should use his services over those of RedSense.

94. REDACTED is another RedSense customer. Prior to Bohuslavskiy's resignation, Bohuslavskiy was supposed to conduct a scheduled briefing with REDACTED. Bohuslavskiy unilaterally cancelled the briefing without explanation, did not reschedule the meeting, and resigned soon after. RedSense is informed and believes, and on that basis allege that, Bohuslavskiy conveniently cancelled the briefing knowing that he was going to resign and knowing that he could use the promise of delivering this briefing as a way to induce REDACTED to retain Bohuslavskiy for the threat intelligence services.

95. Additionally, many of RedSense's largest customers are within the healthcare industry. RedSense's healthcare customers face unique concerns and have heightened sensitivity regarding data protection and preventing breaches of health information. RedSense is aware that many of its customers are members of

Health-Information Sharing & Analysis Center ("Health-ISAC"), which is a non-profit organization that provides a platform for security professionals in the health industry to share insights, best practices, alerts, and intelligence.

96. Based on RedSense's interactions with its customers in the health sector, RedSense is informed and believes, and on that basis alleges, that Health-ISAC is the preeminent industry organization for key players in the industry, such as CISO's of RedSense's healthcare customers. Health-ISAC offers events for its members, including monthly threat briefings.

97. On June 24, 2025, RedSense learned from several of its healthcare customers who had attended the Health-ISAC June Monthly Threat Briefing (that occurred earlier that day), that Bohuslavskiy was a speaker at the briefing and based on the event agenda was speaking as a "representative of RedSense." RedSense partners and leadership did not have any visibility into this speaking engagement. As such, it did not authorize Bohuslavskiy to speak at this event on "behalf" of RedSense or as its "representative" and did not approve any messaging that Bohuslavskiy presented at this event. Multiple RedSense customers who attended this event and had previously received correspondence from Bohuslavskiy reached out to RedSense with confusion. They asked whether Bohuslavskiy was "back at" RedSense and did not understand why Bohuslavskiy was advertised as being a "representative of RedSense." Although RedSense does not have visibility

as to the substance of Bohuslavskiy's speaking engagement, given the tenor of his other communications to the industry and directly to RedSense's customers, RedSense is informed and believes, and on that basis alleges, that he did not "represent" RedSense in a positive light. At minimum, he has further created confusion as he attempts to market his own threat intelligence offering while taking advantage and misusing RedSense's reputation to the detriment of RedSense's customer relationship.

98. Because of Bohuslavskiy's interference with RedSense's contracts, RedSense has suffered the loss of its vital business contracts. Because of the sensitive nature of this industry, it is unlikely that RedSense will ever be able to regain the trust of its customers, which has caused RedSense irreparable harm.

THIRD CAUSE OF ACTION – TORTIOUS INTERFERENCE WITH FUTURE ECONOMIC ADVANTAGE

99. RedSense repeats, realleges and incorporates by references paragraphs 1 through 98 as if set forth herein.

100. RedSense has maintained consistently positive relationships with its major customers year over year, and thus it reasonably expects the maintenance of its business relationships with its customers, including but not limited to: REDACTED

REDACTED RedSense also had an expectation in the growth of its customers based on its high-quality services and the positive reputation that it had within the cybersecurity and threat intelligence industry.

101. In his email smear campaign to RedSense customers, Bohuslavskiy repeatedly indicated that customers should distrust the quality of RedSense's services, and that they should turn to him instead for cybersecurity needs going forward.

102. As the former Chief Research Officer of RedSense, Bohuslavskiy understood RedSense's continuing expectations of relationships with its major customers. By denigrating RedSense's offerings as a cybersecurity provider, Bohuslavskiy understood his interference would likely undermine RedSense's future economic advantages. Further, by presenting as a potential security breach or threat himself, Bohuslavskiy understood that his spam emails to the customers would cause customers to question RedSense's capabilities as a cybersecurity vendor in a manner that diminishes the likelihood that the customers would renew their contracts with RedSense.

103. For example, in at least one instance, RedSense and REDACTED were engaged in serious discussions regarding REDACTED retaining the services of RedSense. Accordingly, RedSense viewed REDACTED as a prospective customer.

These discussions with REDACTED have, since Bohuslavskiy's resignations and public decrying of RedSense, come to a halt. A REDACTED executive revealed to RedSense that there was too much of a cloud over RedSense as a result of Bohuslavskiy's smear campaign and the rumors about Bohuslavskiy and RedSense that have been circulating in the threat intelligence industry. The same executive informed RedSense that unless RedSense is able to resolve this issue, REDACTED would not feel comfortable retaining RedSense's services.

104. Thus, because of Bohuslavskiy's interference with RedSense contracts, RedSense has lost credibility with its current and prospective customers, and as a result, has suffered a loss of reasonably relied-upon future economic advantages.

FOURTH CAUSE OF ACTION – VIOLATION OF THE DEFEND TRADE SECRETS ACT (18 U.S.C. § 1836, *et seq.*)

105. RedSense repeats, realleges and incorporates by references paragraphs 1 through 104 as if set forth herein.

106. RedSense owns the RedSense Trade Secrets.

107. RedSense implements measures that are reasonable under the circumstances to protect the secrecy of the RedSense Trade Secrets. As described herein, RedSense takes steps that are consistent with standard industry practices to ensure the RedSense Trade Secrets are protected.

108. RedSense expended considerable resources to design, develop, create, and implement the RedSense Trade Secrets, which are then implemented into the services provided by RedSense to its customers and leveraged by RedSense to maintain these customer relationships.

109. The RedSense Trade Secrets derive substantial value from secrecy, and they provide RedSense with an important competitive advantage in the marketplace.

110. Bohuslavskiy misappropriated the RedSense Trade Secrets by:

a. Utilizing and leveraging the RedSense Trade Secrets, which includes its customer list, to direct his email smear campaign to the companies who would be most impacted by his denigration of RedSense (*i.e.*, RedSense's current customer and prospective customers).

b. Utilizing the RedSense Trade Secrets, including information regarding RedSense's largest and most valuable customers, to interfere with the customer relationships that would be most critical to RedSense's operation if RedSense lost the relationship.

c. Utilizing and leveraging the RedSense Trade Secrets, which include specific information **REDACTED**

REDACTED to target these customers with specificity and by capitalizing on these REDACTED in connection with his email smear campaign.

d. Utilizing and leveraging the RedSense Trade Secrets regarding the unique and individualized services that RedSense provides to improperly compete with RedSense by knowing which services and features are most critical to RedSense's customers.

111. RedSense has been and will continue to be harmed by Bohuslavskiy's misappropriation, which has also unjustly enriched Bohuslavskiy.

FIFTH CAUSE OF ACTION – FRAUD

112. RedSense repeats, realleges and incorporates by references paragraphs 1 through 111 as if set forth herein.

113. In connection with Bohuslavskiy's role at RedSense (and his belief that he was a partner of RedSense), Bohuslavskiy had authority to approve invoices submitted by the third-party vendors whose work he managed. As a team leader, Bohuslavskiy was also in a position to supervise the use of licensed software and inspect the deliverables supposedly produced by the freelance contractors.

114. RedSense made payments on invoices received from the companies (Affix, Irasel, EasyStaff, and Pyrus) for work that each of these companies

purportedly performed for RedSense. Each of these payments was approved by Bohuslavskiy.

115. To date, RedSense has not received these services, nor the technology promised to them, meaning RedSense has made thousands of dollars in payments and has received nothing in return.

116. Given that Bohuslavskiy managed these vendors and acted on behalf of these vendors (including, *e.g.*, submitting a resignation on behalf of Dmitriev and the EasyStaff freelancers), RedSense is informed and believes, and on that basis alleges, that Bohuslavskiy would create and submit these "third party invoices" to RedSense, approve the invoices, remit payment to Affix (which is solely owned by Bohuslavskiy) for the supposed dispersal of funds to the vendors, but would instead pocket the funds himself.

117. By directly submitting these invoices to RedSense's Accounting Team on Affix paper, Bohuslavskiy was impliedly approving the invoiced amounts and intentionally misrepresenting that the work had been satisfactorily provided to RedSense such that the contractors warranted payment. By submitting invoices to RedSense from his personal LLC, Affix, rather than directly from the vendor, Bohuslavskiy inserted himself as an intermediary and provided cover that would have allowed him to inflate or even invent contractor invoices. Bohuslavskiy could then conceal whether the money was ultimately disbursed to the third-party

vendor or transferred elsewhere for Bohuslavskiy's own personal gain. In reasonable reliance upon Bohuslavskiy as Chief Research Officer and a supposed partner of RedSense, the Accounting Team remitted payment on these invoices. Indeed, because Bohuslavskiy engaged in layers of obfuscation, it was only after RedSense conducted its audit that it learned of the deception.

118. RedSense had made multiple requests for Bohuslavskiy to provide access to the deliverables and an accounting of what these third parties have provided to RedSense. In each instance, Bohuslavskiy denied RedSense's request. To date, RedSense has not received any quantifiable deliverable that would justify the payments, including but not limited to source code, documentation, data sets, original invoices, project roadmaps, task history, or time tracking.

119. Given that it was Bohuslavskiy's responsibility to manage the work performed by EasyStaff, Irasel, and Pyrus (which he did through Affix), this denial of access and accounting negates any claims from Bohuslavskiy that the work was done.

120. Based on Bohuslavskiy's refusal to provide accounting, RedSense is informed and believes and on that basis alleges, that Bohuslavskiy has fraudulently appropriated RedSense funds for his own use.

121. Bohuslavskiy, as manager of these vendors, knew that the work had not been performed or that its deliverables had been withheld from RedSense, and

therefore neither he nor these third parties were entitled to compensation. Bohuslavskiy's deception and misrepresentation regarding the work that was not performed constitutes a material misrepresentation of fact.

122. Bohuslavskiy was entrusted by RedSense to approve these payments for work actually done and to safeguard RedSense funds as a member and Chief Resource Officer. RedSense reasonably believed that the invoices Bohuslavskiy submitted would be legitimate and, at the time payment was remitted, RedSense had no reason to suspect that these invoices existed to conceal or obfuscate Bohuslavskiy's appropriation of RedSense funds. For example, by submitting invoices from Affix (rather than directly from the vendor), Bohuslavskiy was able to approve the payment and then conceal whether the money was disbursed to the vendor or transferred elsewhere for Bohuslavskiy's own personal gain.

123. Bohuslavskiy's submission of invoices on behalf of the third-party vendors was designed with the intent to defraud RedSense, as RedSense relied on the invoices and mistakenly believed it was remitting payment pursuant to valid invoices for work actually performed.

124. As a result of Bohuslavskiy's fraudulent invoicing, RedSense has been harmed because it has made payment for work without ever receiving the work product and, in some instances, has made double payments on fraudulent

invoices because Bohuslavskiy submitted or approved invoices that he knew were duplicates of what had already been paid.

SIXTH CAUSE OF ACTION – CONVERSION

125. RedSense repeats, realleges and incorporates by references paragraphs 1 through 124 as if set forth herein.

126. RedSense owns all rights, title, and interest in and to the following assets and technology: (1) AIDIS (Project Pylon) including all software and documentation; (2) Pyrus platform including all data since inception; (3) EasyStaff Deliverables, including code, data, research, LLM, documentation; (4) Igor Dmitriev's deliverables as stated in the agreement dated August 1, 2023; (5) Forum Scraping code and results to date; (6) OpenCTI instance and all RedSense Threat Intelligence contained therein; and (7) all AdvIntel threat intelligence reports and historical adversary infrastructure intelligence along with the associated data sets, reports and access data All AdvIntel Reports and threat intelligence since inception.

127. RedSense contracted and paid for all rights, title, and interest, and other associated ownership rights in and to the aforementioned assets and technology.

128. Bohuslavskiy has, without authority, taken, absconded with, stolen, and refused to return on demand the property which RedSense owns, and which Bohuslavskiy does not own and has no legal right to.

129. Bohuslavskiy has, without authority, intentionally exercised dominion or control over the property of RedSense as to interfere with RedSense's ownership rights and as to prevent RedSense from realizing the value of the property it owns.

130. RedSense has made multiple demands for the return of such assets and technology from Bohuslavskiy, who has refused. Prior to Bohuslavskiy's resignation, RedSense conducted an asset inventory seeking information from Bohuslavskiy as to the location of the assets for which RedSense had contracted. Bohuslavskiy refused to identify the locations on the RedSense system where these assets were located. Following his resignation, RedSense demanded that the assets be returned to RedSense, and Bohuslavskiy has refused to comply, claiming that RedSense has no legal right to the assets.

131. Bohuslavskiy, consistent with his involvement at RedSense, would have knowledge regarding RedSense's contracts which provide RedSense the right, title, and interest in and to this property. RedSense is informed and believes, and on this basis alleges, that Bohuslavskiy knew he did not have the right to withhold this property from RedSense.

132. Concurrent with the resignation of Bohuslavskiy, part of the RedSense file system was wiped. Based on the credentials used to wipe the system, RedSense is informed and believes, and on this basis alleges that Bohuslavskiy directed, facilitated, or encouraged the file deletion and removal.

133. Bohuslavskiy's absconding with RedSense's property (in the case of the deleted and removed source code) and his refusal to return the property that RedSense is the legal owner of constitutes an unlawful conversion.

SEVENTH CAUSE OF ACTION – UNJUST ENRICHMENT

134. RedSense repeats, realleges and incorporates by references paragraphs 1 through 133 as if set forth herein.

135. The acts of Bohuslavskiy complained of herein constitute unjust enrichment of Bohuslavskiy at the expense of RedSense in violation of common law.

136. Bohuslavskiy has received and retained an impermissible benefit by absconding with property for which RedSense has paid and is the legal owner.

137. Bohuslavskiy has received and retained and impermissible benefit by authorizing payments by RedSense to third party vendors for work that was not performed. RedSense is informed and believes, and on that basis alleges, that Bohuslavskiy used these third-party vendors to obscure that the payments he was

approving were being rerouted to business entities that he owned for his own personal benefit.

138. Bohuslavskiy, in his capacity as Chief Research Officer and his affiliation with RedSense, used RedSense as his personal bank by approving invoice payments for work that he knew he and others had failed to perform. This approval of payments for Bohuslavskiy's personal financial gain is in excess of the payments that Bohuslavskiy has already received from RedSense (either during the time that RedSense believed he was a partner or as compensation for the work performed).

139. His retention of this property and money has allowed him to obtain profits and benefits to which he is not entitled. His retention of this property and money has been to the detriment of RedSense, who still does not have the work it paid for.

140. Retention by Bohuslavskiy of the profits he derived from his malfeasance would be inequitable.

141. RedSense seeks injunctive relief and compensatory and punitive damages in an amount to be proven at trial, including, without limitation, disgorgement of Bohuslavskiy's ill-gotten profits.

EIGHTH CAUSE OF ACTION – THE ONBOARDING AGREEMENT IS VOID AND UNENFORCEABLE AS TO BOHUSLAVSKIY DUE TO A LACK OF CONSIDERATION (28 U.S.C. § 2201)

142. RedSense repeats, realleges and incorporates by references paragraphs 1 through 141 as if set forth herein.

143. Pursuant 28 U.S.C. § 2201, RedSense brings an action for declaratory relief.

144. Pursuant to the Onboarding Agreement, which Bohuslavskiy executed on January 25, 2023, Bohuslavskiy agreed to provide Obligated In-Kind Funding in the form of threat intelligence and intellectual property in lieu of the monetary contribution required to become a partner of RedSense.

145. The other partners of RedSense understood that Bohuslavskiy would provide the AdvIntel threat intelligence reports and historical adversary infrastructure intelligence along with the associated data sets, reports, and access data to RedSense as part of the Obligated In-Kind Funding.

146. Bohuslavskiy represented and warranted that he had the right to provide the Obligated In-Kind Funding, and that no third party could claim any rights with respect to the assets that Bohuslavskiy was obligated to provide as a condition precedent to become a partner of RedSense.

147. For two years following the execution of the Onboarding Agreement, the other partners of RedSense treated Bohuslavskiy as a partner because they

believed he had provided the Obligated In-Kind Funding that Bohuslavskiy was obligated to provide.

148. On March 31, 2025, Bohuslavskiy, in connection with his refusal to return the AdvIntel threat intelligence reports, violated both the Obligated In-Kind Funding provision and the representation and warranty provision of the Onboarding Agreement by admitting that "RedSense definitely has no claim to this IP and any such transfer — if it were even possible — would violate binding agreements," and that "RedSense clearly had no legal entitlement" to the AdvIntel reports.

149. Because the Obligated In-Kind Funding was the consideration Bohuslavskiy was obligated to convey as a condition precedent to becoming a partner, his admission that he never had the right to convey the AdvIntel reports, and in fact never did provide the AdvIntel reports, means that there was a lack of consideration on the part of Bohuslavskiy with respect to joining the partnership.

150. RedSense will be unfairly harmed and Bohuslavskiy will be unjustly enriched if RedSense is forced to perform under the Onboarding Agreement as to Bohuslavskiy and recognize Bohuslavskiy as a partner of RedSense.

151. Accordingly, RedSense seeks a declaration that the Onboarding Agreement is void and unenforceable as to Bohuslavskiy because of lack of consideration on the part of Bohuslavskiy.

NINTH CAUSE OF ACTION – THE ONBOARDING AGREEMENT IS VOID AND UNENFORCEABLE AS TO BOHUSLAVSKIY DUE TO FRAUD (28 U.S.C. § 2201)

152. RedSense repeats, realleges and incorporates by references paragraphs 1 through 151 as if set forth herein.

153. Pursuant 28 U.S.C. § 2201, RedSense brings an action for declaratory relief.

154. Pursuant to the Onboarding Agreement, which Bohuslavskiy executed, Bohuslavskiy agreed to provide Obligated In-Kind Funding in the form of threat intelligence and intellectual property in lieu of the monetary contribution required to become a partner of RedSense.

155. The other partners of RedSense understood that Bohuslavskiy would provide the AdvIntel threat intelligence reports and historical adversary infrastructure intelligence along with the associated data sets, reports, and access data to RedSense as part of the Obligated In-Kind Funding.

156. Bohuslavskiy represented and warranted that he had the right to provide the Obligated In-Kind Funding, and that no third party could claim any rights with respect to the assets that Bohuslavskiy was obligated to provide as a condition precedent to become a partner of RedSense.

157. For two years following the execution of the Onboarding Agreement, the other partners of RedSense treated Bohuslavskiy as a partner because they

believed he had provided the AdvIntel threat intelligence reports that Bohuslavskiy was obligated to provide.

158. On March 31, 2025, Bohuslavskiy, in connection with his refusal to return the AdvIntel threat intelligence reports, violated both the Obligated In-Kind Funding provision and the representation and warranty provision by admitting that "RedSense definitely has no claim to this IP and any such transfer — if it were even possible — would violate binding agreements," and that "RedSense clearly had no legal entitlement" to the AdvIntel reports.

159. To induce RedSense's other partners to grant him partnership rights, Bohuslavskiy represented that he had the ability and right to convey the threat intelligence and intellectual property to RedSense in lieu of the monetary contribution required of other partners.

160. Bohuslavskiy knew that RedSense relied on Bohuslavskiy's representations regarding his right and ability to convey the threat intelligence and intellectual property and would not have granted Bohuslavskiy partnership rights if Bohuslavskiy had not promised the Obligated In-Kind Funding and represented that he could provide the Obligated In-Kind Funding

161. The Obligated In-Kind Funding and representation and warranty provisions were material terms of the Onboarding Agreement.

162. Based on the admissions made in Bohuslavskiy's March 31 letter, RedSense is informed and believes, and on that basis alleges, that Bohuslavskiy knew that, in contravention to the representation and warranty he made in the Onboarding Agreement, that he had no legal right to convey the threat intelligence and intellectual property and knew that such representation was false.

163. RedSense and its other partners relied on the representation and warranty provided by Bohuslavskiy and his promise to convey the Obligated In-Kind Funding. Because RedSense and its other partners believed Bohuslavskiy to be truthful in his representation and warranty and promise to convey the Obligated In-Kind Funding, they allowed him to be a partner of RedSense, provided him with access to proprietary company information that only partners have access to, and entrusted him with management of RedSense as an equal partner.

164. RedSense and its other partners would not have allowed Bohuslavskiy to join the RedSense partnership had they known that his representation and warranty was false and his purported Obligated In-Kind Funding was actually worthless because RedSense would never receive nor have legal right to the threat intelligence and intellectual property that was promised.

165. RedSense will be unfairly harmed and Bohuslavskiy will be unjustly enriched if RedSense is forced to perform under the Onboarding Agreement as to Bohuslavskiy and recognize Bohuslavskiy as a partner of RedSense.

166. Accordingly, RedSense seeks a declaration that the Onboarding Agreement is void and unenforceable as to Bohuslavskiy because of fraud on the part of Bohuslavskiy at the formation of the Onboarding Agreement.

TENTH CAUSE OF ACTION – BREACH OF FIDUCIARY DUTIES (Wyo. Stat. 17-29-409)

167. RedSense repeats, realleges and incorporates by references paragraphs 1 through 166 as if set forth herein.

168. In the alternative, if it is determined that Bohuslavskiy is and was a partner of RedSense pursuant to the Onboarding Agreement, Bohuslavskiy as a partner of RedSense owes fiduciary duties of loyalty and care to the LLC and to the other partners under the Wyoming LLC Act.

169. The duty of loyalty requires Bohuslavskiy to refrain from dealing with RedSense as or on behalf of a person having an interest adverse to RedSense.

170. The duty of loyalty also requires Bohuslavskiy to refrain from competing with RedSense in the conduct of RedSense's activities and business.

171. By advertising his own threat intelligence services to existing RedSense customers for the purpose of diverting the customers away from RedSense, sullying RedSense's reputation, denigrating RedSense's services, and competing with RedSense for this business, Bohuslavskiy violated his duty of loyalty to RedSense.

172. Bohuslavskiy had an obligation to not compete with RedSense and not use proprietary, confidential, and trade secret information belonging to RedSense to usurp the opportunities that RedSense has taken time and care to cultivate.

173. The duty of care requires Bohuslavskiy to act with the care that a person in a like position would reasonably exercise under similar circumstances.

174. By approving invoices for work that had not been performed, by approving duplicate payments, by encouraging his brother and the EasyStaff freelancers not to sign the CIIAA, by failing to attend partner meetings to discuss crucial and critical issues such as the financial condition of RedSense, by ceasing to perform his responsibilities and yet maintaining the illusion that he and his team remained productive, by refusing to provide the intellectual property and assets that RedSense contracted and paid for (and that Bohuslavskiy was responsible for providing), by absconding with RedSense property, by facilitating, directing, requesting, or encouraging the wiping and destruction of the file system containing RedSense source code using credentials that were assigned to Dmitriev, by denigrating the reputation of RedSense to current and prospective customers, by providing false and misleading information to RedSense customers about RedSense, by harassing RedSense customers with multiple spam-like communications, by stealing the proprietary and trade secret information belonging to RedSense, and by encouraging RedSense customers to break their contracts with

RedSense and retain Bohuslavskiy's services instead, Bohuslavskiy failed to act with the care of a reasonable partner of RedSense.

175. All of these acts carried out by Bohuslavskiy were adverse to the best interests of the company and have caused financial and reputational harm to RedSense.

176. Bohuslavskiy has engaged and continues to engage in wrongful conduct as described herein that has adversely and materially affected and will continue to adversely and materially affect RedSense's activities.

177. Bohuslavskiy has willfully and persistently committed and continues to willfully and persistently commit a material breach of his duties under Wyo. Stat. 17-29-409.

178. Bohuslavskiy has engaged in and continues to engage in conduct relating to RedSense's activities which are to the detriment of RedSense, and it is no longer reasonably practical for RedSense to carry on its activities with Bohuslavskiy as a partner.

PRAYER FOR RELIEF

WHEREFORE, RedSense prays that the Court:

a. Enter judgment in favor of RedSense and against Bohuslavskiy.

b. Declare that Bohuslavskiy's conduct has been willful, and that Bohuslavskiy has acted with fraud, malice, and oppression.

c. Enter a preliminary and permanent injunction enjoining Bohuslavskiy from contacting current and prospective customers of RedSense and interfering with the relationships between RedSense and its current and prospective customers, specifically enjoining Bohuslavskiy from the following conduct: (1) publicly or privately soliciting RedSense's current customers and prospective customers[11] for business, (2) publicly or privately denigrating the quality of RedSense's cybersecurity services, (3) publicly or privately using RedSense proprietary or trade secret information or RedSense property that rightfully belongs to RedSense (but that Bohuslavskiy has absconded with) to improperly compete with RedSense, (4) publicly or privately making false statements about RedSense, its products and services for the purpose of stealing the business away from RedSense, (5) publicly or privately making false statements about RedSense not honoring its customer contracts, (6) holding himself out as a representative of RedSense or as someone who is authorized to act on behalf of RedSense at industry events

[11] By virtue of Bohuslavskiy's involvement with RedSense, he was aware of prospective customer relationships. RedSense seeks to limit the injunction with respect to the prospective customers to those relationships that were in the pipeline prior to Bohuslavskiy's resignation or that Bohuslavskiy otherwise had knowledge of.

or via other public platforms, and (7) engaging in speaking engagements where he purports to speak as a representative of or on behalf of RedSense.

d. Require Bohuslavskiy to remove references to continued or ongoing affiliation with RedSense from his social media accounts and other personal marketing materials.

e. Require Bohuslavskiy to remove references to "ethical concerns" at RedSense from his social media accounts.

f. Require Bohuslavskiy return the following property, to which RedSense owns all right, title, and interest and for which RedSense contracted and/or paid: (1) AIDIS (Project Pylon) including all software and documentation; (2) Pyrus platform including all data since inception; (3) Easy Staff Deliverables, including code, data, research, LLM, documentation; (4) Igor Dmitriev's deliverables as stated in the agreement dated August 1, 2023; (5) Forum Scraping code and results to date; (6) OpenCTI instance and all RedSense Threat Intelligence contained therein; and (7) All AdvIntel threat intelligence reports and historical adversary infrastructure intelligence along with the associated data sets, reports and access data since inception.

g. Enter judgment awarding RedSense actual damages from Bohuslavskiy adequate to compensate RedSense for the activities and misconduct of Bohuslavskiy complained herein and for any injury complained herein,

including but not limited to interest and costs, in an amount to be proven at trial.

h. Enter judgment disgorging Bohuslavskiy's profits.

i. Enter judgment awarding enhanced, exemplary, and special damages, in an amount to be proven at trial.

j. Enter judgment awarding attorneys' fees and costs.

k. Order such other relief that the Court deems just and reasonable.

DEMAND FOR JURY TRIAL

RedSense respectfully requests a trial by jury on all issues so triable in accordance with Fed. R. Civ. P. 38.

Dated: June 27, 2025

CROWELL & MORING LLP

By: s/ Preetha Chakrabarti

Preetha Chakrabarti
pchakrabarti@crowell.com
Rachel Elaine Hsu (*pro hac vice* forthcoming)
rhsu@crowell.com
Crowell & Moring LLP
Two Manhattan West
375 Ninth Avenue
New York, NY 10001
Telephone: (212) 223-4000
Facsimile: (212) 223-4134

Anna Z. Saber (*pro hac vice* forthcoming)
asaber@crowell.com
Crowell & Moring LLP
3 Embarcadero, 26th Floor
San Francisco, CA 94111
Telephone: (415) 986-2800
Facsimile: (415) 986-2827

Attorneys for Plaintiff Red Sense LLC